LAW OFFICES OF
FAY KAPLUN & MARCIN, LLP
INTELLECTUAL PROPERTY LAW

150 BROADWAY, SUITE 702
NEW YORK, NEW YORK 10038
PHONE: (212) 619-6000
FAX : (212) 208-6819
WWW.FKMIPLAW.COM

FACSIMILE COVER SHEET

FAX NO	:	(571) 273-8300
TO	:	Commissioner for Patents Mail Stop: Appeal Brief - Patent
FROM	:	Oleg F. Kaplun, Esq. of Fay Kaplun & Marcin, LLP
DATE	:	June 12, 2007
SUBJECT	Re:	U.S. Patent Appln. Serial No. 10/535,327 for *A Method of Distributing the Location Dta of a Mobile Device* Phillips Ref.: GB 020197

NUMBER OF PAGES INCLUDING COVER : 14

MESSAGE:

Please see attached.

IF ANY PAGES WERE NOT RECEIVED OR ARE ILLEGIBLE, PLEASE CALL (212) 619-6000 AS SOON AS POSSIBLE
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us by telephone, and return the original message to us at the above address via the U.S. Postal Service. We will reimburse any costs you incur in notifying us and returning the message to us. Thank you.

Attorney Docket No. US 020197

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Christopher Steel
Serial No.	:	10/535,327
Filed	:	February 6, 2006
Title	:	A Method of Distributing the Location Data of a Mobile Device
Group Art Unit	:	2631
Examiner	:	Amancio Gonzalez
Confirmation No.	:	5733

Mail Stop: Appeal Brief - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Facsimile

I hereby certify that this correspondence is being deposited via facsimile addressed to:

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
Alexandria, VA 22313-1450
571-273-8300

By: Oleg F. Kaplun, (Reg. No. 45,559) Date: June 12, 2007

TRANSMITTAL

In support of the Notice of Appeal filed on April 12, 2007, transmitted herewith please find an Appeal Brief for filing in the above-identified application. Please charge the Credit Card of **Fay Kaplun & Marcin, LLP** in the amount of $500.00 (PTO-Form 2038 is enclosed herewith). The Commissioner is hereby authorized to charge the **Deposit Account of Fay Kaplun & Marcin, LLP NO. 50-1492** for any additional required fees. A copy of this paper is enclosed for that purpose.

Respectfully submitted,

Dated: June 12, 2007

By:
Oleg F. Kaplun, Reg. 45,559

Attorney Docket No. US 020197

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Christopher Steel
Serial No.	:	10/535,327
Filed	:	February 6, 2006
Title	:	A Method of Distributing the Location Data of a Mobile Device
Group Art Unit	:	2631
Examiner	:	Amancio Gonzalez
Confirmation No.	:	5733

Mail Stop: Appeal Brief - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Facsimile

I hereby certify that this correspondence is being deposited via facsimile addressed to:

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
Alexandria, VA 22313-1450
571-273-8300

By:
Oleg F. Kaplan, (Reg. No. 45,559) Date: June 12, 2007

TRANSMITTAL

In support of the Notice of Appeal filed on April 12, 2007, transmitted herewith please find an Appeal Brief for filing in the above-identified application. Please charge the Credit Card of **Fay Kaplun & Marcin, LLP** in the amount of $500.00 (PTO-Form 2038 is enclosed herewith). The Commissioner is hereby authorized to charge the **Deposit Account of Fay Kaplun & Marcin, LLP NO. 50-1492** for any additional required fees. A copy of this paper is enclosed for that purpose.

Respectfully submitted,

Dated: June 12, 2007

By:__________
Oleg F. Kaplun, Reg. 45,559

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In reApplication of:	)	
	)	
Christopher G. Steel	)	
	)	
Serial No.: 10/535,327	)	Group Art Unit: 2617
	)	
Filed February 6, 2006	)	Examiner: Amancio Gonzalez
	)	
For: METHOD OF DISTRIBUTING THE LOCATION DATA OF A MOBILE DEVICE	)	**Board of Patent Appeals and Interferences**
	)	
	)	
	)	

Mail Stop: Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

In support of the notice of appeal filed on April 12, 2007, and pursuant to 37 C.F.R. § 41.37, Appellant presents this Appeal Brief in the above-captioned application.

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 1-4 in the Final Office Action dated January 12, 2007. The appealed claims are set forth in the attached Claims Appendix.

1. Real Party in Interest

This application is assigned to Philips Research USA, the real party in interest.

2. Related Appeals and Interferences

There are no other appeals or interferences which would directly affect, be directly affected, or have a bearing on the instant appeal.

3. Status of the Claims

Claims 1-4 have been rejected in the Final Office Action. The final rejection of claims 1-4 is being appealed.

4. Status of Amendments

No amendments have been submitted by Appellant.

5. Summary of Claimed Subject Matter

The present invention, as recited in independent claim 1, relates to a method of distributing the location of a mobile device. The method comprises determining the location of the mobile device (MS2). (See Specification, p. 3, ll. 13-20; Figs. 1-2.) The determined location is encrypted using an encryption key. (See id., p. 4, ll. 4-8.) The encrypted location is transmitted to a server (IS). (See id., p. 3, ll. 26-30; Figs. 1, 3.) The encrypted location is stored at the server (IS). (See id., p. 4, ll. 4-8; Figs. 1, 3.) A remote terminal (MS1) queries the server (IS). (See id., p. 4, ll. 12-15; Figs. 1-3.) The server (IS) transmits the encrypted location to the remote terminal (MS1) in response to the query. (See id., p. 4, ll. 15-16; Figs. 1-3.) The predetermined encryption key is shared between the mobile device (MS2) and the remote terminal (MS1) but not with the server (IS). (See id., p. 4, ll. 1-3; Figs. 1-3.) The location is decrypted at the remote terminal (MS1) using the predetermined encryption key. (See id., p. 4, ll. 17-19; Figs. 1-2.)

The present invention, as recited in independent claim 2, relates to a mobile device (MS2). The mobile device (MS2) is configured to determine its location. (See id., p. 3, ll. 13-20; Figs. 1-2.) The mobile device (MS2) is further configured to encrypt its location using an encryption key. (See id., p. 4, ll. 4-8; Figs. 1-2.) The mobile device (MS2) is further configured to transmit the encrypted location to a server (IS). (See id., p. 3, ll. 26-30; Figs. 1-3.) The mobile device (MS2) is further configured to share the predetermined encryption key with a remote terminal (MS1) but not the server (IS). (See id., p. 4, ll. 1-3; Figs. 1-3.)

The present invention, as recited in independent claim 3, relates to a server (IS). The server (IS) is configured to receive and store an encrypted location which is encrypted with an encryption key and which corresponds to a mobile device (MS2). (See id., p. 3, ll. 26-30; p. 4, ll. 4-8; Figs. 1-3.) The server (IS) is further configured to transmit the encrypted location to a remote terminal (MS1) in response to a query from the remote terminal (MS1). (See id., p. 4, ll. 12-16; Figs. 1-3.) Between receipt and transmission of the encrypted location by the server (IS), the server (IS) is not in possession of the encryption key. (See id., p. 4, ll. 1-3, 22-23; Figs. 1, 3.)

The present invention, as recited in independent claim 4, relates to a terminal (MS1). The terminal (MS1) is configured to query a remote server (IS) for the location of a particular mobile device (MS2) with which it has shared an encryption key independently of the server (IS). (See id., p. 4, ll. 1-3, 12-15; Figs. 1-3.) Upon receipt of an encrypted location encrypted with the encryption key, the terminal (MS1) is further configured to decrypt the location. (See id., p. 4, ll. 17-19; Figs. 1-2.)

6. Ground of Rejection to be Reviewed on Appeal

I. Whether claims 1-4 are unpatentable under 35 U.S.C. § 102(e) over U.S. Patent 7,013,391 to Herle et al. (hereinafter "Herle").

7. Argument

I. The Rejection of Claims 1-4 Under 35 U.S.C. § 102(e) Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 1-4 under 35 U.S.C. § 102(e) as unpatentable over Herle. (See 1/12/07 Office Action, pp. 3-5.) In the Advisory Action, the Examiner restated the grounds for rejection provided in the Final Office Action. (See 3/20/07 Advisory Action, p. 2, ll. 1-5.)

Herle includes a mobile station location server that determines a mobile station's location through various locating techniques or by receiving the location information from the mobile station over an encrypted channel. The server stores the location in memory that may be accessed by authorized client access devices. A requesting client access device transmits a request to the server. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit the information in either an encrypted or decrypted form to the device. (See Herle, Abstract.) The server also holds within its memory profile fields of the mobile stations, authorized client profile fields, and encryption-decryption keys. (See id., col. 5, ll. 55-57.) Using the different fields and keys, the server authenticates and transmits the location information. (See id., col. 5, l. 59 – col. 6, l. 8.)

B.. Herle Does Not Disclose Sharing the Predetermined Encryption Key Between the Mobile Device and the Remote Terminal But Not With the Server As Recited in Claim 1.

Herle describes a mobile station location server 160 that is shown in detail in Figure 3. (See Herle, col. 5, ll. 32-34; Fig. 3.) The mobile station location server 160 includes a memory 310. (See id., col. 5, ll. 34-35; Fig. 3.) Memory 310 stores operating system 320, position server program 330, client access interface program 340 and mobile station database 350, which contains a plurality of mobile station records 360, 370, 380. (See id., col. 5, ll. 46-52; Fig. 3.) Exemplary mobile station record 360 contains mobile station profile field 361, authorized client profile(s) field 362, and encryption-decryption key(s) 363. (See id., col. 5, ll. 55-57; Fig. 3.)

The server 160, through server application program 330, controls access to mobile station database 360. When a request for position data is received, the server application program 330 determines whether the request contains a proper decryption key. (See id., col. 6, ll. 1-8.) If the request properly authenticates, the requested position data is sent to the requesting client. In one embodiment, the server 160 transmits encrypted position data to an authorized client access device, which then decrypts the position data. (See id., col. 6, ll. 52-56.) In another embodiment, the server 160 decrypts the position data and transmits unencrypted position data to an authenticated client access device. (See id., col. 6, ll. 56-60.)

Herle discloses an embodiment of the server 160 wherein the server *transmits* the position data to the requesting client device in its encrypted form. However, Herle *does not* disclose an embodiment wherein the server 160 does not store encryption-decryption key(s) 363. Nor does Herle disclose any motivation for an embodiment that deliberately hides the encryption-decryption key(s) 363 from the server 160. In contrast, claim 1 specifically recites "sharing the predetermined encryption key between the mobile device and the remote terminal *but not with the server*."

In the Advisory Action, the Examiner noted that Herle discloses "determining the location of a mobile device, storing in a server the encrypted location of said mobile device and then sharing said encrypted data with a second mobile device." (3/20/07 Advisory Action, p. 2, ll. 2-4.) The Examiner does not assert that Herle discloses the limitation "sharing the predetermined encryption key between the mobile device and the remote terminal but not with the server," recited in claim 1, because Herle does not disclose such an embodiment. Accordingly, the rejection of claim 1 over Herle should be overturned.

C. Herle Does Not Disclose a Mobile Device Configured To Share the Predetermined Encryption Key With a Remote Terminal but Not the Server As Recited in Claim 2.

Claim 2 recites "[a] mobile device configured to ... and share the predetermined encryption key with a remote terminal but not the server." Appellant respectfully submits that Herle does not disclose "shar[ing] the predetermined encryption key with a remote terminal but not the server" for the reasons stated above with reference to claim 1. Accordingly, the rejection of claim 2 over Herle should be overturned.

D. Herle Does Not Disclose Wherein Between Receipt and Transmission of The Encrypted Location By the Server, the Server Is Not In Possession of The Encryption Key As Recited in Claim 3.

Claim 3 recites "[a] server configured to receive and store an encrypted location which is encrypted with an encryption key... wherein between receipt and transmission of the encrypted location by the server, the server is not in possession of the encryption key." Appellant respectfully submits that Herle does not disclose a server that "is not in possession of the encryption key" for the reasons stated above with reference to claim 1. Accordingly, the rejection of claim 3 over Herle should be overturned.

E. Herle Does Not Disclose A Terminal Configured To Query a Remote Server For the Location of a Particular Mobile Device With Which It Has Shared an Encryption Key Independently of the Server As Recited in Claim 4.

Claim 4 recites "A terminal configured to query a remote server for the location of a particular mobile device with which it has shared an encryption key independently of the server..." Appellant respectfully submits that Herle does not disclose "shar[ing] an encryption key independently of the server" for the reasons stated above with reference to claim 1. Accordingly, the rejection of claim 4 over Herle should be overturned.

8. Conclusion

For the reasons set forth above, Appellant respectfully requests that the Board reverse the rejection of the claims by the Examiner under 35 U.S.C. § 102(e), and indicate that claims 1-4 are allowable.

Please direct all future correspondence to:

Paul Im, Esq.
Corporate Patent Counsel

Philips Intellectual Property & Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9602
Fax: (914) 332-0615
Email: paul.im@philips.com

Respectfully submitted,

Date: June 12, 2007

By: ______________________
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel.: (212) 619-6000
Fax: (212) 619-0276

CLAIMS APPENDIX

1. (Rejected) A method of distributing the location of a mobile device comprising the steps of:

determining the location of the mobile device

encrypting the determined location using an encryption key;

transmitting the encrypted location to a server;

storing the encrypted location at the server;

querying the server from a remote terminal;

transmitting from the server to the remote terminal the encrypted location in response to the query;

sharing the predetermined encryption key between the mobile device and the remote terminal but not with the server; and

decrypting the location at the remote terminal using the predetermined encryption key.

2. (Rejected) A mobile device configured to determine its location, encrypt its location using an encryption key, transmit the encrypted location to a server, and share the predetermined encryption key with a remote terminal but not the server.

3. (Rejected) A server configured to receive and store an encrypted location which is encrypted with an encryption key and corresponds to a mobile device; and in response to a query from a remote terminal, to transmit to the remote terminal the encrypted location; wherein between receipt and transmission of the encrypted location by the server, the server is not in possession of the encryption key.

4. (Rejected) A terminal configured to query a remote server for the location of a particular mobile device with which it has shared an encryption key independently of the server; and upon receipt of an encrypted location encrypted with the encryption key, decrypting the location.

EVIDENCE APPENDIX

No evidence has been entered or relied upon in the present appeal.

RELATED PROCEEDINGS APPENDIX

No decisions have been rendered regarding the present appeal or any proceedings related thereto.